Consolidated Technology Services • WA

Service Inquiry
Global Address List Synchronization

September 25, 2012

Business Driver

Most Washington State agencies have joined the Enterprise Active Directory (EAD), and the Enterprise Exchange Organization. As a result, they share a Global Address List (GAL) containing contact information for over 60,000 State employees.

Agencies who have not joined EAD, have a need to communicate and work with these same employees. These agencies must either create custom contacts in their own Exchange Organization structures or rely on other methods to find email addresses, phone numbers and locations of state employees. As state employees change jobs or leave the state, keeping these 'shadow' address lists current becomes burdensome.

Global Address List Synchronization (GAL Sync) is a way to automate the creation and maintenance of contacts across Active Directory (AD) and Exchange Organization structures belonging to trusted government entities. Several entities have requested this functionality, namely the Washington State Patrol, Department of Transportation, Legislative Service Center and the Office of the Courts.

Overview and Potential Benefits

Global Address List synchronization can be accomplished by the use of Microsoft's Forefront Identity Manger (FIM) synchronization service. This service uses a 'connector' to keep address lists in separate AD Forests synchronized. It does this without requiring the use of forest trusts. FIM copies mail-enabled contacts into each participating AD environment, representing employees and resources in the other AD environment(s). These are then kept in sync by FIM. Synchronization can be one-way or bi-directional.

Use of FIM will require that participating agencies:

- be joined to the State Governmental Network (SGN)
- open specific agency firewall ports to allow necessary access
- provide an AD service account with read/write access to their AD Forest
- configure their Forest's Domain Name Services (DNS) to enable communications with the FIM Server.

Only one FIM Server is allowed to manage the synchronization across multiple entities. In fact, multiple FIM Servers would result in 'collisions' of objects in the directories. This document assumes a FIM server deployed in the EAD. Connectors are then set up with other agency AD Forests (or other identity stores).

Synchronization can be managed to occur after hours or at specific intervals to reduce network traffic and impact on the AD Forests. Filter lists can be created to limit synchronization of information and objects between connected agencies or to allow agencies to opt-out of synchronization entirely.

CTS Effort to Deploy and Support:

Work to be Completed:

- Design work and a design review for the project
- Configuring FIM in the EAD Pre-production environment and piloting with a customer agency
- Standing up the FIM Synchronization Service in the EAD Production environment, which includes:
    - installing and configuring hardware and FIM software
    - installing and configuring SQL
    - training staff on FIM support
    - creating filter lists for participating agencies
    - working with the customer agencies to set up connectors
    - preparing the AD organization unit (OU) structure for synchronization
    - Creating 'recipient policies' in Exchange to add the new mail-enabled contacts to the GAL

Staffing resources necessary for the project would include Design, Project, Server Provisioning, Network, Security, AD and SQL subject matter experts.

Estimated Time to Implement: 6 - 10 months

Support and Maintenance: Support requirements for the FIM Synchronization Service are estimated at an average of 1 hour per day to maintain logs, create custom filter lists as requested, create new connectors as requested, resolve replication conflicts and failures and general maintenance and monitoring of the environment.

Agency Support Responsibilities:

EAD Agency tasks would include:

- removing any manually created contacts that will now be populated from other agency AD forests via FIM
- work with CTS to create custom filter lists (may need to change their OU structure and move accounts in order to accomplish filtering rules)

Non-EAD Agency tasks would include:

- connect to the SGN (if they are not currently connected)
- create a service account with read/write access to their AD Forest
- work with CTS to establish the synchronization connector

- remove any manually created contacts that will now be populated from EAD via FIM
- create DNS conditional forwarders to enable communication with the FIM Server

User Training: End users need to be educated about the changes they can expect in the Exchange Global Address Lists as a result of synchronization with other agencies and the timing of when synchronizations can be expected to occur.

Estimated Project Effort and Costs:

The estimated project resource effort and cost is 1,194 hours and $88,953.00.

Project Resource Costs:

Project Manager:	350 hours
Design:	200 hours (includes design, design review, cross agency team)
Network:	16 hours
Security:	48 hours
Storage:	16 hours
Server Provisioning:	24 hours
Operations	
Active Directory:	450 hours (2 AD SMEs)
SQL Server:	90 hours

Consulting Costs:

Microsoft Active Directory DSE: 24 Premier Hours @ $250 per hour = $6,000

Total Cost Estimate for Hardware, Software and Support: $5,207.39 per month for the first year and $4,228.73 per month thereafter.

Production System:

Hardware Costs: $2,142.03 per month
Software Costs: $10,601.28 or $978.66 per month for 12 months

Pre-Production Environment:

Hardware Costs: $594.70 per month (2 Virtual Servers (2 Cores, 8 GB RAM))
Software Costs: $1,142.68 (Included in monthly software costs above)

Support Costs: 1 hour per day (.125 of an FTE = $1,492 per month)

Additional Technical Detail:

Two IBM H23 Blades with Dual 8 core processors and 64 GB of RAM, (2) 300 GB HDD and 300 GB of RAID 1 SAN Storage (as recommended by Microsoft).

SQL Server 2012 Standard, Windows 2012 Standard, Forefront Identity Management Server

Microsoft recommends that a FIM Server be configured with 2 to 4 quad-core processors and 32 GB of memory with Windows 2008 R2, Forefront Identity Manger 2010 and SQL Enterprise 2010 installed on the same server.

The recommendation that SQL be installed on the FIM box is for performance reasons. If SQL is located on another Server, it should have a dedicated SQL instance for FIM.

High Availability and Disaster Recovery are accomplished in FIM by using a warm standby server. FIM is installed on the standby with the service turned off and SQL Replication is used to keep the SQL Database up to date. Synchronization of directory data is not a mission critical need and should not require a highly available, site resilient installation. A warm standby would be appropriate for this service. Synchronization can be scheduled after hours daily. The ramifications of the service being unavailable would be that over time the data in the directory would become stale, but it would still exist until the service could be restored.

Microsoft recommends SQL Enterprise 2008 R2 and Windows Enterprise 2008 R2. Pricing is no longer available on the Microsoft Select Contract for those products. If SQL Enterprise 2012 is required, it would cost approximate $64,000.00 for this service for the SQL License per server. Windows Enterprise is no longer available, but the Data Center version would be approximately $64,000 as well per server.